Index Number: AF-2010-7.4
Approval Date: 1/19/2017

Millennium Challenge Corporation Privacy Policy

January 19, 2016
AF-2010-7.4

Submitted by:
Chief Privacy Officer, Policy Owner Department of Administration & Finance
Millennium Challenge Corporation (MCC) 875 15th Street N.W.
Washington, DC 20005

Privacy Policy

	APPROVER:	Mahmoud Bah
		VP of Administration & Finance
Section	**Significant Changes**	
Section 3	Included additional relevant OMB memoranda references.	
Section 4:	Removed this section but incorporated Sensitive PII in Section 6.	
Section 6	Added the definition of Web Measurement and Customization Technology. Added the definition of Sensitive PII.	
Section 8.1	Added examples of SPII.	
Section 8.3	Defined privacy breach to include only SPII.	
Section 8.6	Updated the Conditions of Disclosure.	
Section 10.4.5	Clarification that privacy information is not to be released except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be for the purpose specified in 5 USC § 552a.	
Section 11.2	Added new policies related to web measurement and customization technologies.	
Section 12.4	Outlined the elements of Statement of Record Notices.	

Section 13.2	Removed paragraph on System of Records Disclosure Exemption.	
Section 13.4	Change in the roles and responsibilities of the CEO to clarify requirements under OMB Memorandum 05-04.	
Appendix A	Added Appendix A: Privacy Information – MCC Breach Response and Notification Procedures	
Section 3	Added Federal Information Security Management Act (FISMA) of 2014 (44 USC § 3554), and deleted FISMS 2002; Added NIST SP 800-144; and Added NIST SP 800-53, Rev. 4.	
Section 5	Included Fair Information Practice Principles (FIPPs).	
Section 7.2	Privacy Training	Updated language to include MCC's incorporation of Privacy Training with Cyber Security Training
Section 8.4.b	Added entire section.	
Section 8.5	Updated section to clarify encryption use for outside transmissions.	
Section 8.7	Updated section to clarify encryption requirement for removable electronic media.	
Section 9.14	Updated encryption use and removed requirement to encrypt data at rest.	

Table of Contents

1. SCOPE

This policy is applicable to MCC employees, personal service contractors and all other contractors handling privacy information.

2. OVERVIEW

This document groups security policies into several high-level roles and defines the mandatory requirements for MCC employees and contractors to understand their obligations as set out in this policy. These policies are driven by Public Laws, Executive Orders, regulatory requirements, and OMB directives. This document contains the following policy sections:

a. Enterprise Policies

b. Policies for Custodians

c. Policies for System of Record Owners

d. Policies for the Director of Web Services

e. Policies for the Chief Privacy Officer

f. Policies for the Chief Executive Officer

g. Issue-Specific Policies

3. AUTHORITIES

The primary statutory authorities include:

a. The Privacy Act of 1974 (5 USC § 552a) as amended

b. E-Government Act of 2002 Section 208 (44 USC § 3601, et seq.), Dec.17, 2002

c. Federal Information Security Management Act (FISMA) of 2014 (44 USC § 3554)

d. Paperwork Reduction Act of 1995 (44 USC § 3501 et seq.) May 22, 1995

e. Government Paperwork Elimination Act (44 USC § 3504) as amended, October 21, 1998

f. Consolidated Appropriations Act 2005, Div. H, Title V, Sec. 522 (Pub. L. 108-447), December 8, 2004

The regulatory authorities include:

a. OMB Circular A-130 Appendix I, Section 4a, 4b – Agency Biennial Privacy Act Report and Agency Biennial Computer Matching Report; and Appendix III, Security of Federal Automated Information Resources

b. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 23, 2003

c. OMB Memorandum 05-04, Policies for Federal Agency Public Websites, December 17, 2004

d. OMB Memorandum 05-15, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, June 13, 2005

e. OMB Memorandum 06-15, Safeguarding Personally Identifiable Information, May 22, 2006

f. OMB Memorandum 06-16, Protection of Sensitive Agency Information, June 23, 2006

g. OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

h. OMB Memorandum 06-20, FY2006 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management

i. OMB FY 2007 Instructions for Preparing Federal Information Security Management Act Report and Privacy Management Report

j. Executive Order 13402: Strengthening Federal Efforts to Protect Against Identity Theft, November 3, 2006

k. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

l. OMB Memorandum 10-22, Guidance for Online Use of Web Measurement and Customization Technologies

m. OMB Memorandum 10-23, Guidance for Agency Use of Third-Party Websites and Applications

n. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing

o. NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations

4. ROLES AND RESPONSIBILITIES

The Privacy Act and subsequent statutory and regulatory guidance establish privacy-specific roles and responsibilities, which are described below.

a. The **Chief Executive Officer (CEO)** is responsible for establishing a compliant Privacy Program that aligns with Federal law and Office of Management and Budget (OMB) guidance.

b. The **Chief Privacy Officer (CPO)** is responsible for developing and implementing the MCC Privacy Program and for day-to-day privacy program operations and the creation of privacy plans and procedures.

c. The **Chief Information Security Officer** is responsible for privacy incident response and incident reporting.

d. The **Director of Web Services** is responsible for providing assistance**,** as required by the Chief Privacy Officer**,** in the review of the privacy policies and procedures with respect to public Web sites.

e. The **Office of the General Counsel (OGC)** provides assistance, as required by the Chief Privacy Officer (CPO), in review of reports, Privacy Impact Assessments, systems of records notices, proposed rules, response to breach incidents and other related matters that are submitted to Congress, OMB, and other parties.

5. DEFINITIONS

Custodian **–** Any MCC employee or contractor who handles privacy information in the routine execution of his or her daily work responsibilities.

Disclosure **–** Dissemination or communication of any information that has been retrieved from a record which contains Personally Identifiable Information (PII) or is otherwise protected by any means of communication (written, oral, electronic, or mechanical) with or without written request by or consent of the individual to whom the record pertains.

Encryption **–** The act of transforming information into an unintelligible form, specifically to obscure its meaning or content.

Fair Information Practice Principles (FIPPs) – Principles that guide and enhance the federal agency's approach to universally and consistently apply trusted identities in online transactions.

Individual **–** For purposes of the Privacy Act, a citizen of the United States or an alien lawfully admitted for permanent residence.

Information Collection **–** Obtaining, soliciting, or requiring the disclosure from third parties or the public, of facts or opinions by or for an agency, regardless of form or format. Such collections include requesting responses from ten or more people other than Federal employees or agencies, which are to be used for general statistical purposes. This usage does not include collection of information in connection with a criminal investigation or prosecution.

Information in Identifiable Form **–** Information in an IT system or online collection: 1) that directly identifies an individual (e.g., name, address, social security number, or other identifying number or code, telephone number, e-mail address, etc.) or 2) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Information System (IS) **–** The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. This term includes both automated and manual information systems. {Source: a variation of a term from NSTISSI 4009}

Personal Identifier – A name, number, or symbol that is unique to an individual. Examples are the individual's name and Social Security number, and may also include fingerprints or voiceprints or any other form of biometric data.

Personally Identifiable Information (PII) – Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to MCC. Not all PII is sensitive. For example, information on a business card or in a public phone directory of agency employees is PII, but in most cases not Sensitive PII, because it is usually widely available public information.

Sensitive PII (SPII) - Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements. Examples of such Sensitive PII include: Social Security number (SSN), passport number, or biometric identifier. Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of employee names with poor performance ratings.

Privacy Act Record – Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint or a photograph.

Privacy Act Request – A request from an individual, or his or her legal guardian, for notification as to the existence of, access to, or amendment of records about that individual. These records must be maintained in a system of records.

Privacy Act Statement – A statement appearing on a website or information collection form that notifies users of the authority for collecting requested information. It also states the purpose and use of the collected information. The public or users must be notified if providing such information is voluntary or mandatory, and the effects, if any, of not providing all or any portion of the requested information.

Privacy Impact Assessment (PIA) – Analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in electronic information systems, and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Record – For purposes of the Privacy Act, any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to the individual's education, financial transactions, medical, criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint or a photograph.

Routine Use **–** Regarding disclosure of a record - usage of a record for a purpose which is compatible with the purpose for which it was collected. Routine uses shall be listed in each System of Records Notice.

System Owner **–** The executive sponsor of an MCC system of records and the individual responsible for managing financial and resource allocation.

System of Records **–** A group of any records under the control of MCC from which information is retrieved by name, Social Security number, or other identifying symbol assigned to an individual.

System of Records Notice (SORN) **–** A legal document used to promote transparency and provide notice to the public regarding rights and procedures for accessing and correcting the record maintained by an agency on an individual in a System of Records. For further details on elements of a SORN, see Section 12.4 of this policy.

User – Any MCC employee or contractor who has access to MCC information systems

Web Measurement and Customization Technology – Technology used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis or usage or to customize a user's (site visitor's) experience.

6. PENALTIES AND DISCIPLINARY ACTIONS

Users who either intentionally or negligently misuse privacy information entrusted to them or do not comply with the policies in this document or with the plans, procedures and rules of behavior derived from them, are subject to the full range of administrative disciplinary actions consistent with MCC policy. These sanctions may range from counseling to removal.

It should be noted, that any officer or employee of MCC, who by virtue of his/her employment or official position, has possession of, or access to, MCC records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act, or the rules and regulations promulgated thereunder, who knowingly and willfully discloses the material to any person or agency not entitled to receive it or who willfully maintains a system of records without publishing a SORN, may be guilty of a misdemeanor and subject to a fine of up to $5000. When there is a reason to believe a user's actions appear to be criminal in nature, the matter must be referred to the Office of Inspector General (OIG) and the OGC.

In addition to the actions listed above, the CPO may suspend an individual's access to the privacy information.

7. ENTERPRISE POLICIES

7.1 Protection of Privacy Information

All MCC employees and contractors must protect privacy information in accordance with this and related policies.

Sensitive PII can include, but is not limited to, Social Security Numbers; health records or medical records; employment history; financial data; biometric data (fingerprint, iris scan, or DNA); criminal history; name and mother's maiden name; driver's license number; or date and place of birth.

7.2 Awareness and Training

Privacy awareness training is required so that users understand their roles and responsibilities relating to privacy information and understand MCC privacy policy. Additionally, privacy training enlists the support of the entire organization in the protection of privacy information entrusted to MCC.

Users must receive privacy awareness training prior to being granted access to the MCC network and systems. Therefore, initial privacy awareness training is presented in classroom-style training given to all users as part of the new employee orientation process. Users are only required to attend this classroom training once.

However, all users must complete annual privacy awareness training. Privacy training is incorporated with MCC's annual Cyber Security Training.

7.3 Privacy Breaches

A privacy breach occurs if there is unauthorized access to or collection, use, disclosure or disposal of SPII. The most common privacy breaches occur when PII of customers, clients or employees is lost, stolen or mistakenly disclosed. This includes lost or stolen laptops containing personally identifiable information or mistakenly sending an e-mail containing PII to the wrong person.

All MCC employees and contractors must report suspected privacy breaches to the CPO immediately and follow the procedures defined in the *Privacy Information - MCC Breach Response and Notification Procedures* (see Appendix A).

7.4 Incident Response

MCC management is committed to protecting the privacy information entrusted to the agency from unauthorized access, modification, loss, breach, or other misuse. The MCC security controls reduce the risk of these activities occurring. All MCC employees and contractors must report any potential loss or breach of privacy information immediately to the CPO. The CPO will report confirmed breaches of privacy information to the CISO for incident response. In the event of an incident or an investigation into a possible incident, the MCC CISO, or a designate, is authorized to confiscate or disconnect equipment from the MCC Network.

7.5 Chief Privacy Officer Authority

The CPO can revoke access to privacy information if users do not attend training or upon a user's misuse of or negligence regarding privacy information. The CPO is authorized to require corrective actions for web sites determined to be non-compliant and may shutdown sites until System of Record Owners correct deficiencies.

7.6 Conditions of Disclosure

MCC may disclose privacy information only in accordance with the routine uses described in the applicable System of Records Notice or as otherwise specifically permitted by the Privacy Act, 5 USC 552a(b). Section 552a(b) provides that, no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

a. to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
b. required under the Freedom of Information Act, 5 USC 552;
c. for a routine use as defined and described by 5 USC 552a(a)(7) and (e)(4)(D);
d. to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to law;
e. to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
f. to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
g. to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
h. to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
i. to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
j. to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;
k. pursuant to the order of a court of competent jurisdiction; or
l. to a consumer reporting agency in accordance with 31 U.S.C. Sec. 3711.

8. POLICIES FOR CUSTODIANS

8.1 Privacy Awareness and Training

a. Custodians must:

1. Participate in annual privacy awareness training as provided by the CPO prior to being granted access to any system containing privacy information; and

2. Participate in annual role-based training for employees who are designated custodians who have greater responsibilities for privacy information and handle or process privacy information in the routine performance of their jobs.

8.2 Incident Reporting

a. Custodians must:

1. Report privacy breaches or suspected privacy breaches to the CISO and the CPO.

8.3 Access Agreements

a. Custodians must:

1. Read, agree to, and sign all access agreements prior to being granted access to a system containing privacy information.

8.4 Disclosure

a. Custodians must not disclose any record contained in a system of records by any means of communication to any person, except by written request or prior written consent of the individual to whom the record pertains (or his/her legal guardian) unless one of the 12 conditions for disclosure exists.

b. Authority to grant access to privacy information is limited to OGC

8.5 Transmission and Transfer of Privacy Information

a. Unless one of the 12 conditions for disclosure applies, custodians must:

1. Encrypt privacy information transmitted electronically outside of MCC's Information System using FIPS-compliant cryptographic algorithms; and

2. Send hard copies containing privacy information via an approved means, such as:

(a) US Postal Service;

(b) Army Post Office;

(c) Commercial messenger; or

(d) Unclassified registered pouch.

8.6 Remote Access to Privacy Information

a. Custodians must:

1. Access privacy information remotely only if authorized to do so by the System Owner; and

2. Only use approved MCC two-factor remote access capabilities.

b. Custodians must not:

1. Download privacy information accessed via remote access to any non-MCC device.

8.7 Storage of Privacy Information

a. Custodians must:

1. Where allowable by statute or regulation (e.g. general records schedules issued by the National Archives and Records Administration), protect privacy information under their control during non-duty hours by storing it in a locked office or suite or by securing it in a locked container, such as a file cabinet, or if in electronic form, ensuring that removable media (e.g., CDs, DVDs, and USB drives) is properly encrypted, password-protected and accessible only to employees with an official need to access it.

8.8 Destruction of Privacy Information

a. Custodians must:

1. Destroy documents containing privacy information by shredding or burning; and

2. Sanitize electronic media containing privacy information by following the MCC CISO Media Sanitization Procedures.

9. POLICIES FOR SYSTEM OWNERS

9.1 Privacy Awareness and Training

a. System Owners must, when the system contains privacy records:

1. Ensure that custodians of their system participate in annual role-based privacy training as provided by the CPO; and

2. Ensure custodians are aware of their responsibility to safeguard privacy information within their control.

9.2 Privacy Impact Assessments

a. System Owners must:

1. Conduct Privacy Impacts Assessments of the systems every three years or when a major change occurs;

2. Have all Privacy Impact Assessments approved by the CPO; and

3. Revalidate Privacy Impact Assessments annually.

9.3 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) and subsequent regulatory guidance establish requirements for information collection requests (ICRs). Surveys, questionnaires, registration forms, web sites, and databases may represent information collection requests, and may be subject to the PRA. However, many internal documents requesting this type of information and directed to employees, agencies or instrumentalities of the U.S. government are exempted from PRA.

a. System Owners must:

1. Determine if the system contains surveys, questionnaires, registration forms, web sites, or databases that represent Information Collection Requests that include privacy information; and

2. Submit ICRs to the CPO for review to determine if they require a privacy impact assessment.

9.4 System of Record Notices

a. System Owners must, when the system contains privacy records:

1. Provide documentation in support of System of Record Notice (SORN) publishing to the CPO;

2. Provide documentation in support of SORN publishing to the CPO, if Information Collection Requests contain privacy information;

3. Update SORNs every three years or when a significant change occurs to the information system;

4. Maintain records with accuracy, relevance, timeliness, and completeness to assure fairness to the individual of record;

5. Not permit information collected about an individual for one purpose to be used for another purpose without giving notice or getting the consent of the subject of the record unless the record is being used as a routine use (e.g., those published for the subject SOR), and not permit information about an individual to be released except when pursuant to a written request by, or with written consent from, the individual to whom the information pertains (unless disclosure of this information would be for the purpose specified in United States Code (USC) - 5 USC § 552a).

6. Contact the CPO when planning to modify the System of Record and provide documentation in support of any proposed changes; and

7. Support to CPO with completing an updated SORN.

9.5 Information Security Controls

a. System Owners must:

1. Abide by the MCC Information System Security Policy to ensure appropriate security controls are in place to protect privacy information.

9.6 Collection of Privacy Information

a. System Owners must:

1. Have a defined and documented business purpose for the collection of privacy data elements;

2. Limit the collection of privacy data elements to the minimum required;

3. Maintain only privacy information considered relevant and necessary for the legally valid purpose for which it is obtained; and

4. Where practicable, collect information directly from the individual.

9.7 Notification of Legal Process

a. System Owners must:

1. Make reasonable effort to notify an individual when any record of that individual is made available to any person under compulsory legal process when this process becomes a matter of public record.

9.8 Disclosure

a. System Owners must, when the system contains privacy records:

1. Maintain an accounting of disclosures of privacy records under their control, except for routine intra-agency or FOIA disclosures, that must include:

   (a) Date, nature, and purpose of each disclosure of a record to any person or agency
   (b) Name and address of the person or agency to whom the disclosure was made

2. Retain privacy information disclosure records for a minimum of five years, or the life of the record, whichever is longer;

3. Account for disclosure information to individuals named in the record at his or her request (except for disclosures made as a part of law enforcement activity); and

4. Inform any person or the other agency about any correction or notation of dispute made by MCC of any record that has been disclosed to an individual or agency, if an accounting of that disclosure is made.

9.9 Remote Access to Privacy Information

a. System Owners must:

1. Specifically authorize remote access to privacy information.

9.10 Rules of Behavior

a. System Owners must:

1. Establish rules of behavior for custodians and for persons involved in the design, development, operation, or maintenance of any system of records under their responsibility; and

2. Maintain copies of signed rules of behavior for each custodian where they acknowledge their understanding of their responsibilities for protecting privacy information and the penalties for non-compliance.

9.11 Privacy Breaches

a. System Owners must:

1. Establish procedures for reviewing reported suspected privacy breaches and confirming a breach occurred;

2. Establish procedures for tracking privacy breaches; and

3. Report confirmed privacy breaches to the CISO for incident reporting to US-CERT and incident response support.

9.12 System of Record Certification and Accreditation

a. System Owners must, when the system contains privacy records:

1. Conduct a Certification and Accreditation of any system storing, processing, or transmitting PII to validate that appropriate security controls are applied and operate as intended as defined in MCC's Information System Security Policy.

9.13 Data Quality

a. System Owners must:

1. Exercise due care in assuring that records containing privacy information are accurate, complete, timely, and relevant to MCC purposes.

9.14 Additional Controls Required for PII

a. System Owners must, when the system contains PII:

1. Implement additional security controls to protect SPII from unauthorized access, disclosure, or modification that include at a minimum:

- Encryption of data in transit using FIPS-compliant encryption

10. POLICIES FOR THE DIRECTOR OF WEB SERVICES

10.1 Compliance Activities

a. The Director of Web Services must:

1. Report annually to the CPO on compliance with Section 208 of the E-Government Act of 2002 to include the following:

- List all systems or information collections for which a PIA was made publicly available (posted on MCC Privacy page, Federal Register, or other site);
- Report on the progress of implementing machine readability technology associated with public web sites; and
- Verify that MCC privacy policy pages on publicly-accessible web sites contain code that enables accessibility devices to automatically read the policy.

10.2 Web Measurement and Customization Technologies

a. The Director of Web Services must:

1. Detail in the agency Public Website Privacy Policy, if using web measurement and customization technology:

(a) the purpose of the web measurement/technology;
(b) the usage tier, session type, and technology used;
(c) the nature, purpose and use of information collected;
(d) whether and to whom the information will be disclosed;
(e) privacy safeguards applied to this information;
(f) data retention policy for this information;
(g) whether the measurement/technology is enabled by default or not and why;
(h) how to opt-out of the web measurement/customization technology;
(i) a statement to site visitors that opting-out still permits users to access comparable information and/or services, and;
(j) identification of all third-party vendors involvement in any web measurement and/or customization technology process.

10.3 Third Party Websites

a. The Director of Web Services must:

1. Examine the third-party's privacy policy with the MCC CPO to evaluate the risks and determine whether the website or application is appropriate for use by the agency before using a third-party website; in addition, the Director of Web Services should then periodically (annually, at a minimum) review the third-party's web site privacy policy for changes that may be made and reassess risks of use.

2. Ensure alerts are provided to visitors, when links are posted leading visitors of the official government domain (www.mcc.gov) to another location, explaining that visitors are being directed to a nongovernment website that may have different policies from those of the MCC's website.

3. If embedding or incorporating a third-party application on the MCC website or other official agency domain, disclose the third-party's involvement with the agency and describe these activities in the Web Privacy Policy.

11. POLICIES FOR THE CHIEF PRIVACY OFFICER

11.1 Privacy Program Development and Oversight

a. The CPO must:

1. Develop and maintain oversight of the Privacy Program in compliance with all applicable statutory and regulatory guidance;

2. Maintain overall custody of protected records and data; and

3. Maintain a list of principle MCC privacy contacts' names and titles for annual reporting.

11.2 Privacy Awareness Training

a. The CPO must:

1. Establish and provide annual privacy awareness training to all employees; and

2. Provide targeted, role-based training to employees who are designated Custodians who have greater responsibilities for privacy information and handle or process PII in the routine performance of their jobs.

11.3 Privacy Impact Assessments

a. The CPO must:

1. Assist System Owners with conducting PIAs

2. Review and approve all Privacy Impact Assessments; and

3. Publish all approved Privacy Impact Assessments on the MCC public website.

11.4 System of Record Notices

a. The CPO must:

1. Publish System of Records Notices in the Federal Register.
   (a) A SORN shall be published in the Federal Register upon establishment or revision of a system of records. The SORN shall include: the name and location of the system; the categories of individuals on whom records are maintained in the system; the categories of records maintained in the system; each routine use of the records contained in the system, including the categories of users and the purpose of such use; MCC's policies and practices

regarding storage, retrievability, access controls, retention, and disposal of the records; the title and business address of the MCC official who is responsible for the system of records; MCC procedures whereby an individual can be notified at his/her request if the system of records contains a record pertaining to him/her; MCC procedures whereby an individual can be notified at his/her request of how to gain access to any record pertaining to him/her contained in the system of records and how to contest its content; and the categories of sources of records in the system.

11.5 Public Web Site Monitoring

a. The CPO must:

1. Monitor public web sites to ensure compliance with privacy requirements.

11.6 Privacy Requests and Appeals

a. The CPO must:

1. Coordinate with OGC to Process Privacy Act inquiries and requests;

2. Establish and implement procedures to track and report privacy requests;

3. Establish and implement procedures to support the amendment of records by individuals for records pertaining to them maintained by MCC; and

4. Establish and implement an appeals process, in coordination with the Offices of General Counsel.

11.7 Privacy Breaches

a. The CPO must:

1. Establish and implement a breach notification plan and procedures where the procedures address:
(a) Whether breach notification is required;
(b) Timeliness of the notification;
(c) Source of the notification;
(d) Contents of the notification;
(e) Means of providing the notification;
(f) Who receives the notification: public outreach in response to a breach, and;
(g) Remedial steps.

2. Review reports of potential breaches and, if confirmed, report the breach to the MCC CISO.

11.8 Information Collection Requests

a. The CPO must:

1. Review all Information Collection Requests (ICRs) to determine if a privacy impact assessment is required.

12. POLICIES FOR THE CHIEF EXECUTIVE OFFICER

12.1 Chief Privacy Officer Designation

a. The CEO must:

1. Designate a Chief Privacy Officer (CPO) who reports to the CEO for Privacy Program matters, and has delegated authority to oversee the program.

12.2 Breach Response Team

a. The CEO must:

1. Establish a Breach Response Team that includes, at a minimum, the CIO, CPO, and OGC.

12.3 Authorization to Create a MCC Web Presence outside of the .gov domain

a. The CEO must:

1. Approve any official participation in hosting MCC content on third-party websites or use of third-party applications.

13. ISSUE-SPECIFIC POLICIES

13.1 Public Websites

a. Web privacy policies must comply with OMB privacy-related memoranda and include notice about the nature, purpose, use, and sharing of information on Federal web sites.

b. All public web sites must prominently display a Privacy Act statement that informs visitors:

1. Of the purpose and use of the collected information, if providing the information is voluntary or mandatory, and the effects, if any, of not providing all or any portion of the requested information;

2. How they grant consent for the use of information they provide on the web site;

3. Of their rights under the Privacy Act or other privacy laws;

4. If collected information is maintained or retrieved by a personal identifier in a system of records; and

5. What information is gathered automatically (e.g., visitor IP address, location, time or visit), and for what purpose the information is gathered (e.g., site management, security).

c. Use clear language to describe MCC practices of protecting information and safeguards used to identify and prevent attacks on the site's information and systems.

d. Any web site that provides content to children under the age of 13 and collects privacy information from these visitors must incorporate requirements of the "Children's Online Privacy Protection Act" (COPPA) in its privacy policy.

e. MCC public web sites must be configured to alert visitors when they are leaving the MCC website for an external, non-.gov website.

f. Any non-MCC website using the MCC logo, such as an MCA website, must clearly indicate that the website is not managed by MCC and not bound by U.S. Government regulations regarding visitor privacy.

14. RELATED MCC PRIVACY PROCEDURES

a. MCC Procedures for Implementing the Privacy Act and the Privacy Provisions of the E-Government Act of 2002.

b. Privacy Information - MCC Breach Response and Notification Procedures (see Appendix A).

Appendix A

PRIVACY INFORMATION - MCC BREACH RESPONSE AND NOTIFICATION PROCEDURES

1 PURPOSE

Following the guidance outlined in the Office of Management and Budget (OMB) memorandum M-07-16, the Millennium Challenge Corporation (MCC) has developed these Privacy Information Breach Response Procedures to minimize the risk to MCC employees and others and to ensure prompt and appropriate action is taken should a breach of personally identifiable information (Breach) occur. In addition to establishing an agency response team, the OMB memorandum recommends that MCC develop a comprehensive Breach notification policy that addresses the following six elements:

a. Whether Breach notification is required;
b. Timeliness of the notification;
c. Source of the notification;
d. Contents of the notification;
e. Means of providing the notification; and
f. Who receives the notification (public outreach in response to a Breach).

This procedure supports current requirements for reporting and handling incidents pursuant to the Federal Information Security Management Act of 2002, the Privacy Act of 1974, the National Institute of Standards and Technology Computer Security Handling Incident Guide, and the concept of operations for the United States Computer Emergency Readiness Team.

2 DEFINITIONS

a. ***Personally Identifiable Information (PII)*** – Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to MCC. Not all PII is sensitive. For example, information on a business card or in a public phone directory of agency employees is PII, but in most cases not Sensitive PII, because it is usually widely available public information.

b. ***Sensitive PII (SPII)*** - Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements. Examples of such Sensitive PII include: Social Security number (SSN), passport number, or biometric identifier. Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of employee names with poor performance ratings.

c. ***Breach*** means loss of control; compromise; unauthorized disclosure, acquisition, or access; or any similar term referring to situations in which persons (other than authorized users and for other than authorized purposes) have access or potential access to PII, whether physically or electronically.

d. ***Incident*** is an event in which a loss of data occurred that may or may not include PII.

3 MCC RESPONSE TEAMS

Consistent with OMB memorandum M-07-16, MCC has created two Breach Notification Response Teams. The MCC response teams' mission is to provide advance planning, guidance, in-depth analysis, and recommendations as to a course of action in response to a Breach. MCC response teams' responsibilities include determining how to respond to a Breach and effective communication to notify affected individuals. The nature and possible impact of the Breach will determine if MCC's Initial Agency Response Team or MCC's Full Agency Response Team needs to be involved.

3.1 Initial Agency Response Team

The initial group that determines if a Breach occurred includes:

a. The manager of the program experiencing the Breach (or responsible for the Breach if it affects more than one program or office);
b. Chief Information Security Officer;
c. A member of the Chief Privacy Officer's team; and
d. A member of the Office of General Counsel.

The Initial Agency Response Team will examine the scope of the information breached, the possible impact breached information will have on individuals and MCC, and whether the Full Agency Response Team needs to be convened.

3.2 Full Agency Response Team

Core members include MCC's:

a. Chief Information Officer (Chair);
b. Chief Privacy Officer (Co-Chair);
c. Chief Information Security Officer;
d. A member of the Office of General Counsel;
e. The Chief Investment and Risk Officer, or a designee thereof;
f. Vice President, Department of Congressional and Public Affairs; and
g. Vice president of the department experiencing or responsible for the Breach.

3.3 Responsibilities of the Response Teams

a. The **Chief Information Officer (CIO)** serves as the chair of the Full Agency Response Team, presides over meetings, and initiates responses to incidents as appropriate.

b. The **Chief Privacy Officer (CPO)** serves as co-chair of the Full Agency Response Team. If the CPO and CIO are the same person then the Chief Information Security Officer (CISO) will service as the co-chair of the Full Agency Response Team. The CPO, or a member of the CPO team, provides subject-matter expertise and operation support in analyzing and responding to a suspected or actual Breach.

c. The **Chief Information Security Officer (CISO)** serves as chair of the Initial Agency Response Team, provides subject matter expertise, and, for example, may provide information on the detection and forensic examination results relating to the incident. The CISO is responsible for participating in all phases of the MCC's planning, preparation, investigation, and response to Breaches involving PII.

d. The **Office of General Counsel (OGC)** is responsible for providing legal support and guidance in responding to a suspected or actual Breach. The OGC member will provide advice as to whether referral of a Breach to other authorities is warranted pursuant to applicable law, regulations, and MCC policies.

e. The Chief Investment and Risk Officer (IRM Representative) provides overall guidance as to agency concerns and risk management issues.

f. The **Vice President for Congressional and Public Affairs (VP-CPA)** develops and communicates appropriate information about the Breach, MCC's response to the public, and addresses media inquiries.

g. The **vice president of the department experiencing or responsible for the Breach** provides the response teams with information and other assistance to address and respond to the Breach.

h. If MCC suspects the Breach was intentional or willful, the matter will be referred to the Office of he Inspector General (OIG) for investigation. The OIG has authority to initiate an investigation of any suspected PII breach no matter how the OIG becomes aware of the suspected Breach.

4 PROCEDURES

4.1 Initial Notification of Breach

a. In the event of a suspected or known Breach, an employee or contractor will promptly notify MCC's Help Desk.

b. Upon notification of the incident, the Help Desk will immediately contact the CISO.

4.2 Convening the Response Teams

In the event of a Breach, the CISO will:

a. Report the incident to the United States Computer Emergency Readiness Team. As required by OMB memorandum M-07-16, all incidents involving PII will be reported within one hour of discovering the incident, which may involve PII that is in either electronic or physical form; and

b. Notify members of MCC's Initial Agency Response Team. The Initial Agency Response Team will, as appropriate, convene a meeting of the Full Agency Response Team, or specific members, as needed.

4.3 Initial Assessment

The Initial Agency Response Team will evaluate available information to determine whether data have been compromised or potentially compromised and how to respond. As part of the initial assessment, the Initial Agency Response Team will address the following information:

a. Date and time of the incident;
b. Date and time the incident was reported;
c. Person who discovered the incident;
d. Person who reported the incident;
e. Nature or circumstances of the incident and means by which the Breach occurred;

f. Description and nature of the data lost or compromised;
g. Storage medium from which data was lost or compromised (*e.g.*, laptop, computer, Blackberry, printed paper);
h. Counter measures enabled when the breach occurred (*e.g.*, full encryption on a computer or laptop, file encryption on certain files on a computer or laptop);
i. Potential remedial steps that can be taken to ameliorate the effects of the Breach and to prevent further Breaches, including the cost and benefit of those steps;
j. Appropriate notice required to affected individuals and other stakeholders; and
k. Number of individuals potentially affected.

The initial assessment will also determine whether the Full Agency Response Team needs to be convened. The Full Agency Response Team will be convened if more than 50 individuals are potentially affected by the Breach; if there is a high risk of harm to affected individuals; if the Breach is likely to require congressional or media communications; or if the costs of MCC's remedial efforts are significant.

4.4 Investigation Responsibilities

Investigation responsibility refers to determining and documenting root causes for the Breach, including:

a. If the MCC response teams determine the Breach involved unintentional loss of control or disclosure of PII, the response teams will have primary responsibility for overseeing the investigation.

b. If an incident appears to involve intentional disclosure of PII, the matter should be immediately referred to the OIG for investigation.

4.5 Risk of Harm Analysis

Consistent with the Privacy Act and OMB memorandum M-07-16 to determine whether notification of a breach is required, MCC response teams will assess the likely risk of harm caused by the Breach, including harm to reputation or potential for harassment or prejudice, particularly when health or financial information is involved. MCC response teams shall consider the following factors:

a. Nature of the data elements breached and context of the data;
b. Number of individuals affected;
c. Likelihood that the information is accessible and usable;
d. Likelihood that the Breach may lead to harm; and
e. Ability of MCC to mitigate risk of harm.

4.6 Notification

a. **Notification to Affected Individuals.** If MCC response teams determine that there is a risk of harm, they will notify affected individuals of the Breach and address the following elements in the notification process:

1. **Timing of Notification.** Notification of a Breach will be provided to affected individuals without unreasonable delay. MCC response teams may decide to delay notification if immediate notification would increase the risk of harm to any affected individual. In such cases, notification may be delayed until appropriate safeguards are put into place.

2. **Source of the Notice.** The source of the notice will be clearly described as originating from MCC; the CPO, in consultation with OGC and the CISO, will originate the notice.

3. **Content of the Notice.** The content of the notice to affected individuals will include the following:

   (a) A brief description of what happened;

   (b) To the extent possible, a description of the type of data involved in the Breach (*e.g.*, full name, social security number, date of birth, home address, account number) and a statement of whether the information was encrypted or protected by other means;

   (c) Steps individuals should take to protect themselves from identity theft or other potential harm; and

   (d) Steps MCC has taken to investigate the Breach, to mitigate losses, and to protect against further Breaches.

4. **Method of Notification.** The appropriate method of notification will depend on the number of affected individuals and the urgency with which notification is required. Possible methods include telephone, first class mail, and e-mail.

b. **Notification to Third Parties.** MCC response teams will carefully coordinate third party notification with notification to affected individuals, including timing, order, and content of the notice. This coordination will ensure that any ongoing investigations are not compromised, the risk of harm to affected individuals is minimized, and the information provided is consistent and accurate. Based on the nature of the Breach, third party notification may be considered to the following:

   1. **Media and the Public.** The VP-CPA, in coordination with MCC response teams, is responsible for directing discussions with the news media and the public, including issuing press releases and posting materials to MCC's website.

   2. **Financial Institutions.** If a Breach involves government-authorized credit cards or individuals' bank account numbers, MCC response teams will promptly notify the bank that handles that particular transaction.

   3. **Appropriate Members of Congress.** The VP-CPA, in coordination with MCC response teams, is responsible for coordinating all communications and meetings with members of Congress and their staff, as necessary.

5 DOCUMENTATION

MCC response teams will document each incident, response plans, and actions taken. This information will be used to track the management and disposition of specific Breaches. The CPO will ensure maintaining adequate and appropriate records to document responses to Breaches. In accordance with the Privacy Act of 1974, MCC response teams will generate, compile, and maintain records to safeguard the financial, legal, or other rights of individuals potentially affected by the Breach.